CHANNEL AND SPECTRUM ESTIMATION FOR SOFTWARE DEFINED RADIO

Connor D. Sanchez, Vincent R. Radzicki, and Hua Lee
University of California, Santa Barbara
Department of Electrical and Computer Engineering
Santa Barbara, CA, 93106
c_d_s@ucsb.edu

Faculty Advisor:
Hua Lee

7/13/2019

ABSTRACT

Software defined radios are rapidly increasing in both research and commercial usage for many different applications. As the number of deployed systems increase, a difficult problem that remains is efficient usage of the Radio-Frequency (RF) spectrum to be shared among all these devices. Two key tasks for the radio to perform here include spectral estimation of the RF environment and channel estimation of the communication channel for which the data will be transmitted. These two steps are linked as the communication channel can change over different portions of the RF-spectrum. In this work, an algorithmic approach is presented for passive and active channel estimation procedures for wideband software-defined radios. The algorithm is comprised of first channel quality estimation followed by communication channel planning to optimize the overall performance.

INTRODUCTION

In many common scenarios, the sensors for a system are competing for communication resources. For example, WiFi routers in an office building. If every company has their router occupying the same channel, then they will all be competing for the same bandwidth. Ideally, one would cooperate with neighboring transceivers so that they no longer share the same resources. What if there is no way to control the environment around our transceiver? Furthermore, what if the environment is adversarial? These are the problems that Cognitive Radio tries to solve. Cognitive Radio attempts to rapidly estimate environmental parameters on a resource limited communication channel and adapt accordingly.

SOFTWARE DEFINED RADIOS FOR SECURE WIRELESS COMMUNICATIONS

The concept of Software Defined Radio (SDR) has been investigated and explored in the research community for decades now, with significant progress being made in realizing the technology's early potential [1]. Recently, a large portion of the development has come from the commercial sector, reducing the cost and increasing the availability of the technology. However, even with this rapid advancement, adoption of SDRs for many applications has been slow [2]. In the telecommunications industries, the current cost is still not competitive enough with traditional Radio Frequency (RF) communication architectures built around RF Application Specific Integrated Circuits (ASIC) devices. One area of need that has recently been identified is secure and reliable point-to-point wireless communication links, which operate in adverse or hostile environments. The advanced functionality and adaptability of SDRs make them well-suited to this challenge, as well as justify their increased cost over conventional radio architectures.

An SDR describes any device that communicates data wirelessly, in where the transmission and reception scheme can be defined programmatically through a software interface, all the way from waveform generation to the data-encoding level. This basic concept is described in a block diagram shown in Fig. 1, where all the digital processing is controlled through the computer. The notion of an SDR is usually credited to Mitola, who believed the concept could revolutionize radio systems engineering [3]. It is true that at that time, and to a large extent now, the only mechanism to add new features or modes to a radio communication system was to introduce and integrate a completely new chipset into its RF-front end. Major changes to a system's hardware are expensive in terms of design resources and cost, difficult to implement, and simply do not scale well [4]. An SDR, in contrast, could in a more reasonable matter be re-programmed to be compatible with new modulation schemes as standards evolve, or operate in different frequency bands to satisfy various spectral emissions regulations. Along with adapting to new wireless standards over time, modern SDRs can dynamically adjust their waveform parameters (shape and frequency) in between transmitting and receiving of data packets in *real-time* as well. The dynamic adjustment of waveform features is what allows SDRs to transmit data securely and discreetly over wireless-links [5].

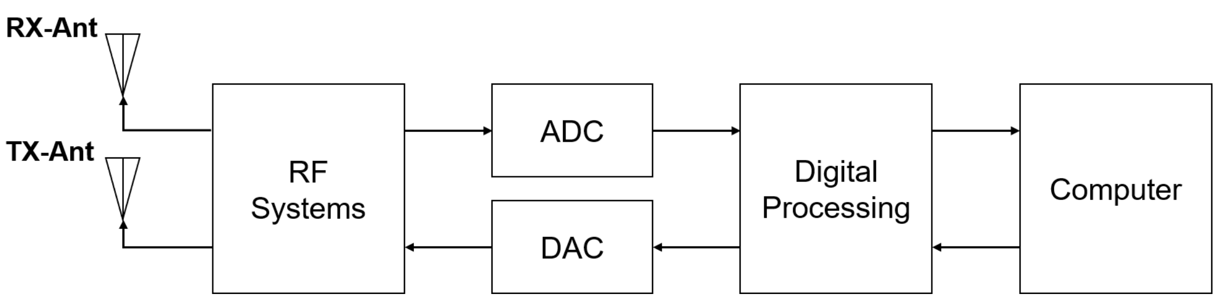

Figure 1: Software-Defined Radio Block Diagram

As wireless communications has become more prevalent and available, many networks have also become more susceptible to adverse attacks and outages. The fixed specifications of wireless communications systems make them easy targets for jamming or interception by adverse actors. For fixed systems, when a security vulnerability is detected and a solution is identified, upgrading deployed systems may be extremely costly if not impossible. However, an SDR can easily be updated through software to patch any security flaws. Additionally, the amount of RF-emitting devices populating the spectrum from both the commercial and security sector is extremely high, as seen in an illustration of the crowded spectral environment shown in Fig. 5. A small SDR can be configured to actively scan the RF environment to identify and avoid these interferers and security threats, like active jammers and spoofing [6].

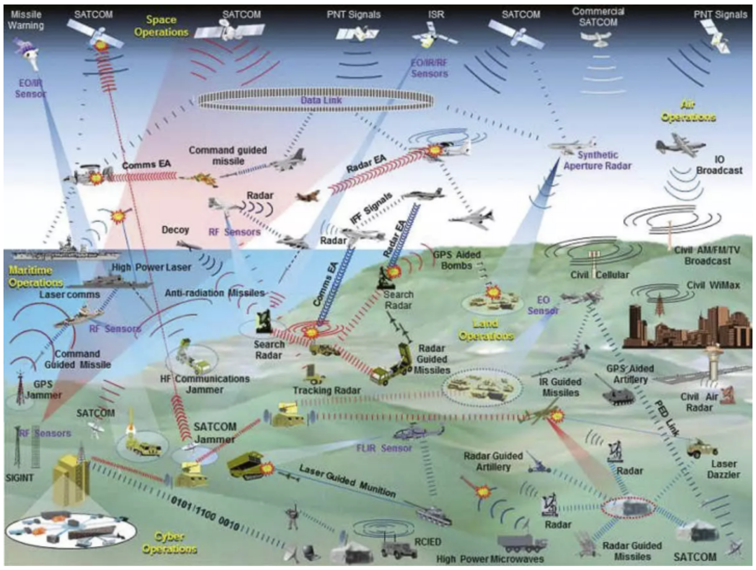

Figure 2: RF Emitting Devices and Modern Spectral Environment [7]

Maintaining a secure, reliable, and robust high-speed, wireless data link in dense RF environments is a challenging task. Secure links are typically required to transmit Low-Probability of Detect (LPD) and Low-Probability of Exploitation (LPE) waveforms, so as to ensure that adverse actors are unable to intercept, capture, and exploit any data sent over the link. Additionally, the system must be reliable and resistant to both unintentional and intentional (jamming) RF-interference. Designing systems for both these scenarios is difficult because the system requirements to achieve both goals are often opposed to one another in fundamental ways [8]. For example, an LPI/LPE waveform is usually small in signal-power, with few distinct features to avoid detection. However, communication systems in a noisy RF environments typically employ large amounts of power and identifiable waveform characteristics to overcome the interference and separate signals from noise. The only feasible way forward to address these challenges is a communications architecture that is able to adapt its waveform and operating frequency in response to real-time measurements.

Modern software-defined radios are capable of achieving this goal, however, careful consideration and thought must be placed when designing the radio system. The most important features an SDR must employ for secure and reliable communication applications include: *RF spectrum sensing* to characterize the RF-environment in real-time, *dynamic waveform generation* for adapting waveform features to the current environment, and *wideband frequency agility* so that the SDR can navigate over different operating bands to avoid detection and exploitation. Characterization of the RF-spectrum by the SDR will help determine the optimal frequency channels and waveform modulation to securely transmit data given the measured interference statistics. LPD/LPE waveforms can be generated dynamically via techniques that ensure the spectral characteristics are spread over the transmit spectrum (Spread Spectrum) to ensure robustness. Frequency agility allows the SDR to change the waveform's carrier frequency over a wideband of operation (Frequency-Hopping), however, determining the optimal rate and pattern of frequency hopping is still an open area of research [9].

In this work, we present our approach to the spectrum estimation and frequency planning portion of the design, and discuss a few of the main issues that need to be addressed. This allows us to focus on open problems in communications and spectrum management, from a software level. The work here can also be developed and applied partially independent to waveform modulation, provided hardware characteristics meet operating requirements. Recent work in intelligent systems and machine learning can also be leveraged to provide new insight and solutions to these problems.

RADIO-FREQUENCY SPECTRUM ESTIMATION AND FREQUENCY-AGILE COMMUNICATIONS SYSTEM

Two subsystems are required for achieving low bit-error rates and a fast frequency hopping rate. The first is a rapid method for estimating the spectral density in each of the channels within our allocated bandwidth. The second is a robust channel switching policy. In an adversarial environment, estimating the spectral density allows our target system to react accordingly. The faster we can detect increased traffic on a channel, the faster we can make the decision to hop carrier frequencies. When the system decides it must switch channels, then it must choose the most advantageous channel that minimizes or maximizes some predefined metric. This metric, taking the spectral density and other channel parameters as input, can be hand crafted to get the desired system behavior. For example, if we want the lowest bit-error rate, then our channel switching policy will always try to be on the channel with the minimum SNR.

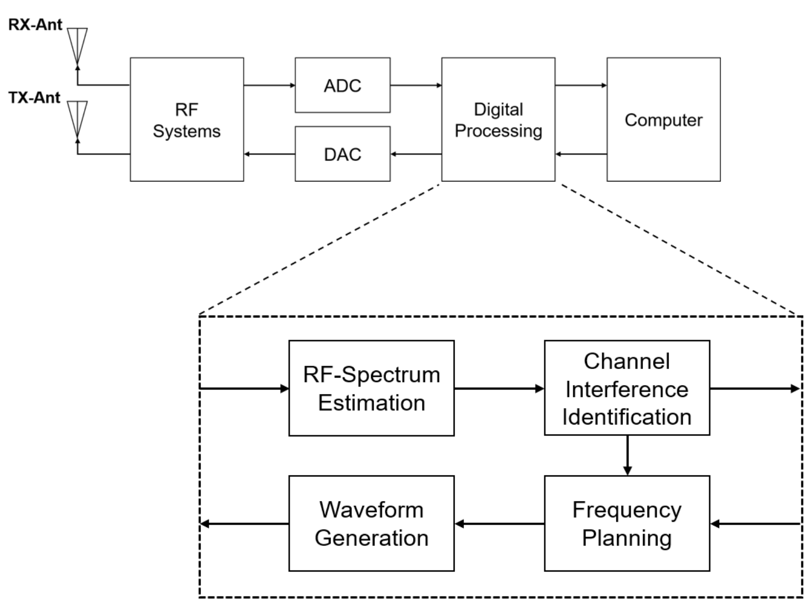

Figure 3: SDR-Based RF-Spectrum Estimation and Frequency Planning Subsystems

The SDR architecture is amenable to implementation of this simultaneous spectrum-estimation and frequency-channel planning scheme proposed here. In Fig. 3, we show where this processing can be implemented on the digital componentry of the SDR system that we discussed in the previous section. The digital receiver can estimate the RF spectrum, and identify channels with high levels of interference. This information can then help the digital transmit chain determine what channels to use and then craft the frequency-hopping plan accordingly. The computing power and resources available on modern SDRs is capable of performing these tasks while also keeping up with the high communication data-rates the radio demands.

For those familiar with reinforcement learning, this system formulation sounds a lot like the Actor-Critic model [10]. These models follow a scheme in which actions are taken according to a certain policy (in this case frequency planning), and the main goal is to find a policy that maximizes some reward (low error-rate). A block diagram of this model can be seen in Fig. 4, where the metric for evaluating the frequency-channel policy is the Bit-Error rate.

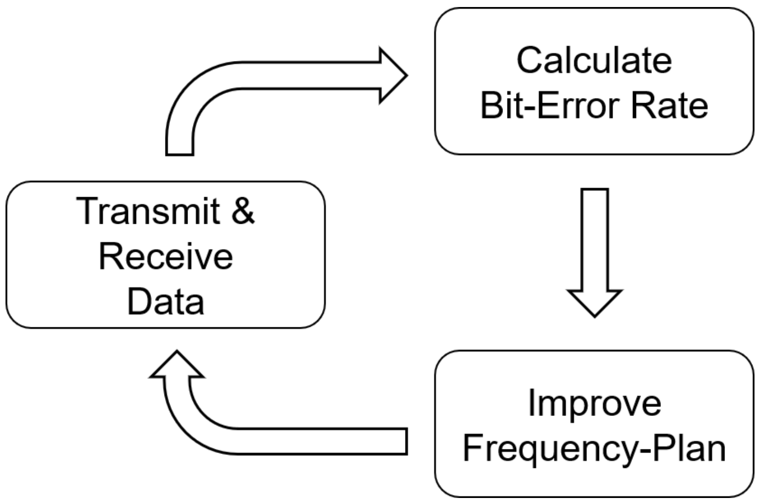

Figure 4: Actor-Critic Reinforcement Learning Model

One key issue that needs to be addressed is the time-frequency resolution problem in RF-spectrum estimation. To maximize performance, the SDR should be able to operate over a wide-portion of RF-Spectrum. Most commercial SDR systems are frequency-agile over a very wide bandwidth (6 GHz), yet their instantaneous measurement bandwidth is limited to the order of MHz due to ADC specifications. High-resolution frequency measurements are desirable for identification of RF-interference and jamming, but they require moderate to long measurement times. This in effect, limits the SDR receiver to only be able to measure small-portions of the overall RF-spectrum for a given measurement time-period. To overcome this, an SDR will typically scan over the full frequency spectrum one small band at a time, but can never fully-characterize the entire RF-band at once. This problem is illustrated in Fig. 5, where (a.) shows a plot of the true distribution of the RF-spectral energy over time and frequency, and (b.) shows the portions of the spectrum that are actively measured. As the RF-environment is changing, there is a possibility that certain inteferers will not be detected, and would not be properly accounted for by the planning algorithm. It is therefore important that the learning model employ flexibility to continuously update the frequency planning based on other metrics, like Bit-Error rate as proposed earlier.

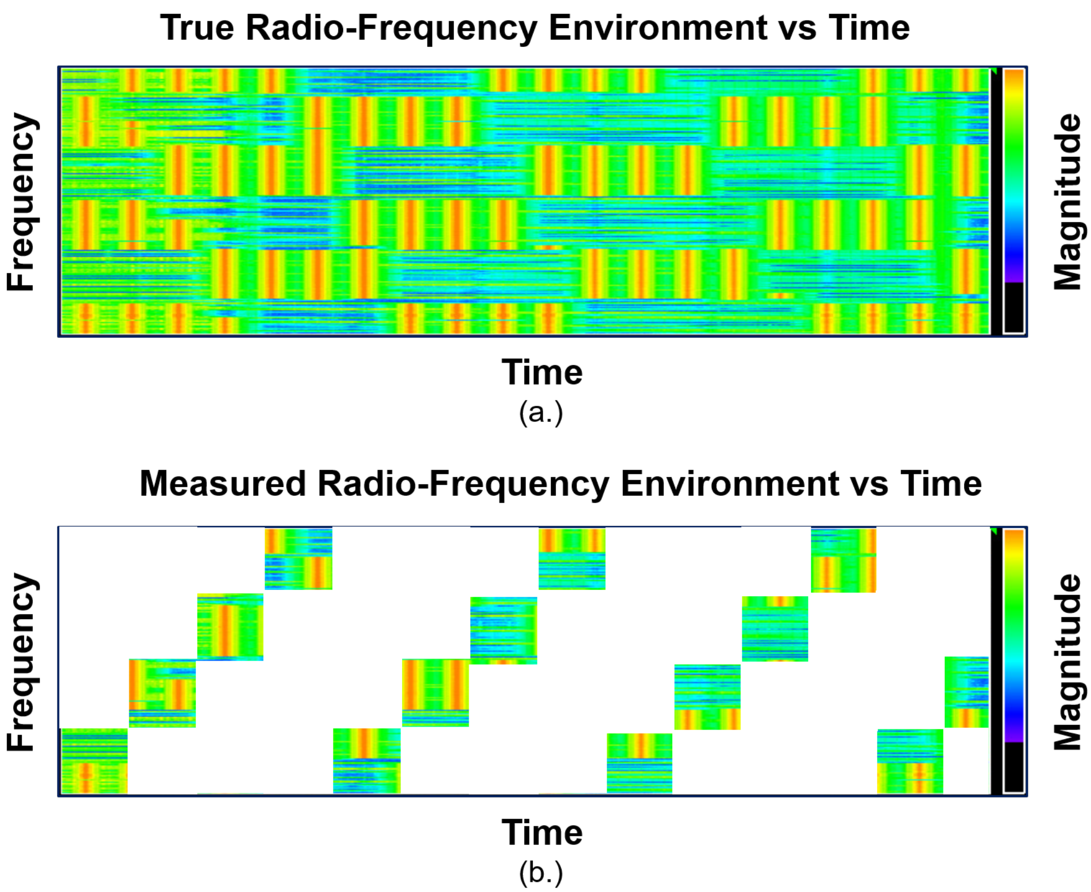

Figure 5: Radio-Frequency Spectral Environment vs Time: The true background environment (a.) and the measured environment (b.) available to the SDR

CONCLUSIONS

In this paper, we describe a methodology for secure, high data-rate communications using Software-Defined Radios. The key performance factors and characteristics of SDRs are identified in the context of their historical developments and modern commercial implementations. Research areas and some of the current problems facing secure, SDR communications are then explored. Specifically, we discuss the issue of joint spectrum estimation and frequency-channel planning, and desribe why SDRs are uniquely suited to address this problem. Lastly, we present a learning-based approach to solving this and outline how it can fit into current SDR architectures. Future work will focus on simulation modelling of the environment and communications systems, and the development of numerical methods for training the proposed algorithms.

REFERENCES

[1] J. Bard and V. J. Kovarik Jr, *Software defined radio: the software communications architecture*, vol. 6. John Wiley & Sons, 2007.

[2] L. Goeller and D. Tate, "A technical review of software defined radios: Vision, reality, and current status," in *2014 IEEE military communications conference*, pp. 1466–1470, IEEE, 2014.

[3] J. Mitola, "Software radios," *IEEE Communications magazine*, vol. 33, no. 5, pp. 24–25, 1995.

[4] A. A. Abidi, "The path to the software-defined radio receiver," *IEEE Journal of Solid-State Circuits*, vol. 42, no. 5, pp. 954–966, 2007.

[5] G. Baldini, T. Sturman, A. R. Biswas, R. Leschhorn, G. Godor, and M. Street, "Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 355–379, 2011.

[6] E. Schmidt, Z. Ruble, D. Akopian, and D. J. Pack, "Software-defined radio gnss instrumentation for spoofing mitigation: A review and a case study," *IEEE Transactions on Instrumentation and Measurement*, 2018.

[7] "Joint air power competence centre." https://www.japcc.org/electronic-warfare-the-forgotten-discipline/. Accessed: 2019-07-13.

[8] L. Turner, "The evolution of featureless waveforms for lpi communications," in *Proceedings of the IEEE 1991 National Aerospace and Electronics Conference NAECON 1991*, pp. 1325–1331, IEEE, 1991.

[9] R. Bell, "Maximum supported hopping rate measurements using the universal software radio peripheral software defined radio," in *Proceedings of the GNU Radio Conference*, vol. 1, 2016.

[10] V. R. Konda and J. N. Tsitsiklis, "Actor-critic algorithms," in *Advances in neural information processing systems*, pp. 1008–1014, 2000.